REMARKS/ARGUMENTS

Favorable reconsideration of this application is respectfully requested.

Claims 1, 4, 6, 14, 16-25, 27-32, 34-37, and 39 are pending in this application. Claims 7-9, 15, 26, 33, 37, and 38 are canceled by the present response without prejudice. Claims 2, 3, 5, 8, and 10-13 were previously canceled without prejudice. Claims 1, 4, 6, 7, 9, 14, 16-20, 22-25, 27-32, and 34-38 were rejected under 35 U.S.C. § 102(b) as anticipated by U.S. patent 5,751,805 to Otsuki et al. (herein "Otsuki"). Claims 15, 21, 26, and 33 were rejected under 35 U.S.C. § 103(a) as unpatentable over Otsuki in view of U.S. patent 4,484,025 to Ostermann et al. (herein "Ostermann"). Claim 39 was rejected under 35 U.S.C. § 103(a) as unpatentable over Otsuki in view of U.S. patent 5,081,679 to Dent.

Addressing the above-noted rejections, those rejections are traversed by the present response.

Initially, applicants note each of the independent claims is amended by the present response to clarify features recited therein. Specifically, independent claim 1 is amended by the present response to incorporate limitations from canceled dependent claim 15. The other independent claims 4, 24, 31, and 39 are similarly amended. That is, the independent claims now recite an encryption unit configured to encrypt a message with the encryption algorithm and send the encrypted message to a second terminal. With reference to Figure 1 in the present specification as a non-limiting example, the terminal unit 20 includes an encryption and decryption device 24 that sends an encrypted message to another terminal. As the claim amendments amend the claims to recite subject matter already pending in the present application, the claim amendments are not believed to raise any issues that would preclude entry of the present amendment after the outstanding Final rejection of April 5, 2005.

Previously pending dependent claim 15, which is now similar in scope to each of the pending independent claims, was rejected based on Otsuki in view of Ostermann. That basis

for the outstanding rejection, however, is believed to be improper as it does not properly consider each of the features recited in the claims.

Amended independent claim 1 is directed to an encryption algorithm management system that includes a terminal unit and a center unit each having a common cipher-key. The terminal unit includes, *inter alia*, an encryption controller configured to renew the common cipher-key in case of receiving encrypted data from the center unit and to decrypt an encryption algorithm from a ciphered encryption algorithm, and an encryption unit configured to encrypt a message with the encryption algorithm and send the encrypted message to a second terminal. Amended independent claim 4 and independent claim 31 are directed to a terminal unit including similar features and independent claim 24 is directed to a system having a terminal unit including similar features.

In a non-limiting example, applicants' Figures 1 and 2 show an encryption algorithm management system including a center unit and a terminal unit that share a common cipher-key Kt. The terminal unit 20i in this example includes an encryption algorithm controller 23 (e.g., encryption controller) that decrypts an encryption algorithm Al from ciphered encryption algorithm E2(KAl)[Al]. The decrypted encryption algorithm Al is used by an encryption and decryption controller 24 to encrypt a message M sent to another terminal unit. The center unit 10 in this example includes an encoder 14 that encrypts a cipher-key KAl for a ciphered encryption algorithm E2(KAl)[Al] with the renewed common cipher-key Kt, and transmits the encrypted data E1(Kt)[KAl] to the terminal unit. A controller 11 in the center unit 10 inputs a state value t into a stream cipher 12, which produces a renewed common cipher-key Kt based on the state value t each time a renewed cipher-key is required (e.g., upon demand or when encrypted data is received). The same state value t is also stored in the terminal unit 20i.

In this example, the user goes to the center for a cipher-key and the cipher-key that is sent form the center changes each time. In particular, t (the state value) of [Kt] changes. In other words, on the first occasion, it is K1, on the second occasion it is K2, etc...

In other words, Figures 1 and 2 show an example of an embodiment of the present invention in which it is necessary to obtain encryption data from a center unit 10 when the encryption algorithm decryption cipher-key is updated. Thus, the encryption algorithm that is employed in the encryption algorithm using system can be managed and dishonest use of the encryption algorithm can be prevented. The encryption algorithm controller 23 is in a memory region that is incapable of being rewritten from outside the terminal (e.g., PC, etc...) and whose contents cannot be read. Therefore, making it possible to prevent tampering by a malicious third party. The controller 11 checks for the existence of the right to use the encryption algorithm by the terminal unit 20i. Then, if the right to use exists, updating the state value t in the stream cipher 12 thereby providing management of the encryption algorithm.

In addition, the non-limiting embodiment of Figures 3 and 4 shows a similar system. However, in the embodiment of Figures 3 and 4, encryption data of the encryption algorithm (e.g., encrypted data E2(Kt)(Al)) is sent by the center unit 10a instead of the encryption data of the decryption cipher-key. At the terminal unit 20ia a request is sent to the center unit 10 on every nth use of the encryption algorithm. A counter 32 is included in the encryption algorithm management unit 30. The encryption algorithm management unit 30 is in a memory region that cannot be rewritten from outside the terminal (e.g., PC, etc...) and whose contents cannot be read, thereby making it possible to prevent tampering by a malicious third party, as in the embodiment of Figures 1 and 2.

In other words, encrypted data E2(Kt)(Al) is used with cipher-key Kt to produce Al (decryption result), but decrypting encrypted data E2(kt)[Al] with cipher-key Kt+1 produces

random data as the decryption result when the counter 32 indicates n or more. Further, the algorithm to be encrypted Al and cipher-key Kij are used to produce encrypted data E(Al, Kij)[M] from message M, in general.

In addition, the non-limiting embodiment of Figures 5 and 6 shows a similar system. However in the embodiment of Figures 5 and 6, the terminal unit makes a decryption request to the center unit 10 on each occasion that the decryption cipher-key has been used n times. The cipher-key information memory 21b, cipher-key information management unit 40, first cipher-key decryption controller 42, and second cipher-key decryption controller 45 are newly provided. The encrypted data E1(ki)[Kij] of the cipher-key Kij and the encrypted data E1(kt)[KAl] of the decryption cipher-key are memorized. Hence, when the counter 43 indicates n or more, random data is the decryption result. Accordingly, dishonest use of the encryption algorithm is prevented by management of the encryption algorithm used in the encryption algorithm system.

Accordingly, the user must receive the data (message) together with the decryption cipher-key sent to the user from the center. Thus, dishonest use by an imposter user, who does not have the decryption cipher-key, can therefore of course not be performed. Further, a surcharge can be required even if a genuine user performs use more than a prescribed number of times (e.g., necessary number of times). Thus, this arrangement advantageously allows management of encryption algorithms and prevention of unauthorized use of encryption algorithms by periodically renewing a common cipher-key in both terminal unit and center unit and sending either a cipher-key for the encryption algorithm or a ciphered encryption algorithm to the terminal unit from the center unit.[1]

Otsuki describes a data-protecting system that includes a software supplier (e.g., center unit) that encrypts a program P with a random number K to produce an encrypted

[1] Specification at page 10, line 5, to page 11, line 9.

program P'.[2] Further, in Otsuki the software supplier encrypts the random number K using an encryption key Kpu (e.g., common cipher-key) to produce an encrypted key K',[3] and sends the encrypted key K' and encrypted program P' to the user (e.g., terminal unit).[4] In Otsuki, the user decrypts the encrypted key K' using another encryption key Kup (e.g., common cipher-key) and decrypts the encrypted program P' based on K.[5] Otsuki does not describe how the encryption key Kpu is generated, but only shows that in Figs. 2 and 3 Kpu appears to be a function of a program password PIN-P and user identifier IDu. Further, Otsuki indicates that encryption key Kup is arithmetically obtained by a loader based on the secret algorithm and the identifier of the user or program,[6] but is silent regarding any way to renew encryption keys Kup and Kpu. Further, Otsuki is silent regarding any means for the user to demand that encrypted data be received from the software supplier (e.g., center unit). Further, Otsuki has no possibility for the user to decrypt an encryption algorithm to then use to send an encrypted message to another terminal.

In such ways, Otsuki is not directed to a device even similar to the claimed features in which a terminal unit decrypts a received encryption algorithm and uses that encryption algorithm to actually encrypt a message to be sent to another terminal. Stated another way, in Otsuki the user terminal does not use an encryption algorithm from the software supplier to output an encrypted message to another terminal. Otsuki is not even similarly related to the claimed features.

Moreover, no teachings in Ostermann overcome the above-noted deficiencies in Otsuki. More particularly, Ostermann is also not at all directed to a device in which a terminal unit needs to decrypt a received encryption algorithm to encrypt a message to be provided to another unit. That is, Ostermann does not teach or suggest any operation in

---

[2] Otsuki at column 5, lines 3-9.
[3] Otsuki at Figs. 2 and 3, and at column 5, lines 22-25, and column 6, lines 48-51.
[4] Otsuki at column 5, lines 37-38.
[5] Otsuki at column 4, lines 5-10 and lines 41-44.
[6] Otsuki at column 6, lines 38-40.

which, as an example, terminal 1 needs to decrypt a received encryption algorithm from a central unit to encrypt a message to be sent to terminal 2. Thus, no combination of teachings of Ostermann in view of Otsuki can meet the limitations of the currently pending amended claims.

In specifically addressing the features as recited in previously pending dependent claim 15 the outstanding Office Action states:

> Otsuki discloses the distribution of ciphered encryption algorithms in a software environment, but not a communications environment. Ostermann discloses a system of enciphered communications between a first and second terminal (Fig. 1) wherein a control center stores a plurality of encryption algorithms that are sent to the terminals so that they may perform secure communications using the same algorithm (Col. 1, lines 46-67).[7]

However, applicants respectfully submit the above-noted basis for the outstanding rejection does not fully consider all of the positively recited claim limitations. As noted above, in the claims an encrypted encryption algorithm is sent from a center unit to a terminal unit. The terminal unit must decrypt that encrypted encryption algorithm and use the encryption algorithm to encrypt a message to be sent to another terminal. Thus, in the claimed invention the terminal unit receives an encrypted encryption algorithm that it must decrypt. That feature is neither taught nor suggested by either Otsuki or Ostermann, and thus no combination of teachings in Otsuki and Ostermann will meet that claimed feature.

First, Otsuki clearly shows in the figures therein the user receiving an encrypted encryption key K', an encrypted program P', and an encrypted second encryption key E(r). However, Otsuki does not disclose or suggest receiving any type of encryption algorithm from the software supplier that the user must then decrypt and utilize to send an encrypted message to another terminal.

[7] Office Action of April 15, 2005, page 6, prenumbered paragraph 11.

Similarly, Ostermann does not teach or suggest such features. More particularly, in Figure 2 Ostermann discloses a system in which a control center 30 includes a cipher program storage 34 that can provide cipher programs to a programmable cipher computer 12 and cipher equipment 16. However, Ostermann also differs from the claims in that Ostermann does not teach or suggest any operation in which the encryption algorithm provided is itself encrypted. In the claims the terminal unit must decrypt the encryption algorithm from the ciphered encryption algorithm with a cipher-key. Ostermann clearly does not each or suggest any such operation.

Further, one of ordinary skill in the art would not and could not have combined the teachings of Ostermann to Otsuki in the manner suggested in the Office Action. Otsuki is directed to a system in which a software supplier provides an encrypted program to a user. Otsuki is not directed to a device in which the user has any need or desire to send an encrypted message to another terminal. Otsuki is directed to a device in which the user merely decrypts the received message.

Further, Ostermann discloses an opposite operation as claimed. Ostermann specifically discloses that "[a] condition which the system must satisfy is that the various code programs per se need not be kept secret, are permitted to be made public and in part can even be publicized..."[8] Thus, Ostermann discloses a system in which the encryption algorithm is to be made public. Ostermann goes on to note that the main feature in the invention is that a key be kept secret.[9]

In contrast to Ostermann, in the claims the encryption algorithm provided from the center unit is itself encrypted and must be decrypted by the terminal. Such an operation is contrary to the above-noted feature in Ostermann of making the code programs public.

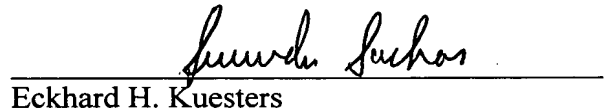
[8] See Ostermann at column 3, lines 63-65.
[9] Ostermann at column 4, lines 1-4.

In such ways, no combination of teachings of Ostermann in view of Otsuki meets the limitations of amended independent claims 1, 4, 24, 31, and 39, and the claims dependent therefrom.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters
Registration No. 28,870
Surinder Sachar
Registration No. 34,423
Attorneys of Record

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)
SNS:smi
I:\ATTY\SNS\19's\198274\198274US-AM 06-03-05.DOC